TRANSMITTAL LETTER
(General - Patent Pending)

Docket No.
L741.01104

In Re Application Of: **Yves AUDEBERT, et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/880,795	June 15, 2001	Linh LD Son	45532	2135	6672

Title: **METHOD, SYSTEM AND APPARATUS FOR A PORTABLE TRANSACTION DEVICE**

COMMISSIONER FOR PATENTS:

Transmitted herewith is:

In response to the Notice of Non-Compliant Appeal Brief dated March 30, 2006, the Appellants hereby submit an Amended Brief, in triplicate, which is in full compliance with 37 CFR 41.37.

in the above identified application.

- ☒ No additional fee is required.
- ☐ A check in the amount of is attached.
- ☒ The Director is hereby authorized to charge and credit Deposit Account No. **19-4375** as described below.
  - ☐ Charge the amount of
  - ☒ Credit any overpayment.
  - ☒ Charge any additional fee required.
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **May 1, 2006**

James E. Ledbetter, Esq.
Registration No. 28,732

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

_____.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Appeals and Interferences

In re the Application of

Inventors: Yves AUDEBERT et al.

Appln No.: 09/880,795

Filed: JUNE 15, 2001

For: METHOD, SYSTEM AND APPARATUS FOR A PORTABLE TRANSACTION DEVICE

APPEAL BRIEF

On Appeal From Group Art Unit 2135

James E. Ledbetter

STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, NW, Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 408-5100
Facsimile: (202) 408-5200

Attorney for Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the present application, ActivCard, of Suresnes Cedex France.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-71 have been presented for examination. Claims 1-39 have been canceled. Claims 40-71 are pending, stand finally rejected, and form the subject matter of the present appeal.

IV. STATUS OF AMENDMENTS

The amendment filed after the final rejection of July 27, 2005, has been entered for the purpose of appeal.

V. SUMMARY OF THE SUBJECT MATTER CLAIMED

Independent claim 40 defines a data processing system for performing authentications and business transactions. The system, as illustrated in Figs. 2A and 2B, includes: (1) a local client 210 that supports a network connection, (2) an authentication server 200 that performs a predetermined authentication policy and supports a network connection, and (3) an intelligent portable

device 100 that supports a personal security device (PSD) 145, a device connection 230, and a network connection 225 (specification page 11, line 32, through page 12, line 2, and page 12, lines 13-20). PSD 145 is functionally connected to intelligent portable device 100 and generates authentication information according to the predetermined authentication policy, which is associated with an identified user (page 7, lines 25-28). Local client 210 and authentication server 200 are functionally connected to each other over a network connection 250 (page 11, lines 32-37). The predetermined authentication policy is functionally stored within PSD 145 and authentication server 200 (page 12, lines 4-11, and page 13, lines 30-34). The local client comprises an activator of an authentication according to the authentication policy between the PSD and the authentication server upon an action of the identified user on the local client (page 7, lines 25-28).

Independent claim 53 defines a method for performing authentications and business transactions. The method includes networking an intelligent portable device 100 that functionally supports connecting a personal security device (PSD) 145 to an authentication server 200 using a network connection (Figs. 2A and 2B and specification page 11, line 32, through page 12, line 2, and page 12, lines 13-20). A shared predetermined authentication policy is functionally stored in authentication server 200 and PSD

145 (page 12, lines 4-11, and page 13, lines 30-34). An authentication request is initiated on a local client 210 by an identified user associated with PSD 145 (page 7, lines 25-28). The request is sent to authentication server 200 through a network 250 connecting local client 210 and authentication server 200 (page 11, lines 32-34), and the identified user is authenticated using the predetermined authentication policy between PSD 145 and authentication server 200 (page 13, lines 30-34). Successful authentication allows the identified user to access the network for additional transactions (page 13, lines 32-34).

Independent claim 65 defines an intelligent portable data processing device 100 for performing authentications and business transactions. As illustrated in Fig. 1A, intelligent portable data processing device 100 has a user interface 140, a display 140, a data processing means 130, a data storage means 135, a device connection 125, and a network connection 105, 110, 115, and 120 (specification page 7, line 31, through page 9, line 24). A personal security device (PSD) 145 associated with an identified user generates authentication information according to a predetermined authentication policy that is shared with a remote authentication server 200 (page 7, lines 25-28). Device 100 has a means 50, 100, 105, 110, 115, 120, 125, 130, and 135 for transferring to PSD 145 a request for authentication with

authentication server 200 using the shared predetermined authentication policy if the request contains an identifier of the user (page 7, lines 25-36).

The references above to the specification and drawings are for illustrative purposes only and are not intended to limit the scope of the invention to the referenced embodiments.

VI. ISSUES

Whether claims 40-58, 60-62, and 64-71 stand correctly rejected under 35 U.S.C. §102(e) as anticipated by Sigaud (US 6,657,956). Whether claim 63 stands correctly rejected under 35 U.S.C. §103(a) as unpatentable over Sigaud. Whether claim 59 stands correctly rejected under 35 U.S.C. §103(a) as unpatentable over Sigaud in view of Boyles et al. (US 6,738,901).

VII. GROUPING OF CLAIMS

For purposes of this appeal, the Appellants hereby state that claims 40-64 stand or fall together, claims 65-71 stand or fall together, and claims 40-64 stand or fall separately relative to claims 65-71.

However, the Appellants respectfully note that the above statement regarding the grouping of claims is made solely for purposes of this appeal and should not be construed as an admission by the Appellants that claims 41-64 and claim 66-71 do not provide a separate and independent basis for their individual allowability relative to that of their base claims.

VII. ARGUMENT

It is submitted that the claimed subject matter defined by each of independent claims 40, 53, and 65 is not anticipated by the applied art.

A. Rejections of Claims 40-52

To anticipate a claim, an applied reference must disclose every element and its identical arrangement with all other elements as defined in the claim. See MPEP §2131, last paragraph; *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); and *Richardson v. Suzuki Motor Co.*,

868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The Appellants respectfully submit that Sigaud fails to disclose at least the feature recited in claim 40 of a local client that activates an authentication operation, according to an authentication policy shared and stored by a PSD and an authentication server, upon an action of a user on the local client.

Sigaud discloses in Fig. 1 a client-server system that provides client-station access to an application server 30 and 31 for a user possessing an authorized portable user object 22 and knowledge of a personal identification number (PIN) associated with portable user object 22. To gain access to application servers 30 and 31, the user inserts his portable user object 22 (e.g., a personal security device (PSD)) into a reader 21 and types his PIN on an input terminal of user station 2. A security processor 1 interposed between user station 2 and application servers 30, 31 cooperates with user station 2 to authenticate the user's PIN and corresponding information obtained from the user's portable user object 22 (see Sigaud abstract). Upon being authenticated, the user may access an application on application server 30 and 31, via user terminal 2, that is authorized by his personal account.

Claim 40 distinguishes over Sigaud's disclosure in that the claimed authentication policy is shared and stored by a PSD and an

authentication server and executed by these two devices upon an action of an identified user on a local client. By contrast, Sigaud discloses a shared authentication policy executed by a local client and an authentication server upon an action of an identified user on the local client.

The Advisory Action proposes that Appellants incorrectly mapped the claimed features to those disclosed by Sigaud in traversing the final rejection applied to claim 40 (see Advisory Action section 2, lines 4-16). The Advisory Action further proposes that a correct mapping of the claimed features to Sigaud's disclosure in Fig. 1 requires: (1) the claimed local client to be mapped to Sigaud's security processor 1, which the Advisory Action denominates as a computer station (section 2, lines 7-8), (2) the claimed authentication server to be mapped to Sigaud's application server-1 30 (section 2, line 8), and (3) the claimed intelligent portable device, containing a PSD, to be mapped to Sigaud's user station 2 (section 2, lines 9-10). The Appellants disagree for the following reasons.

Sigaud discloses that security processor 1 dialogues with one or more user stations 2 in a network and each of the user stations 2 is equipped with a reader 21 for reading chip cards or PCMCIA cards 22 (Sigaud col. 3, lines 29-34). Additionally, Sigaud discloses that security processor 1 is interposed at the junction

of server-1 30 through server-N 31 and located within the same enclosure as servers 30 and 31 so as to protect these servers (col. 3, lines 25-28).

Accordingly, the Advisory Action's proposed mapping necessarily controverts the claimed limitations. Sigaud repeatedly characterizes server-1 30 and server-N 31 as being remotely located with respect to the user stations 2 (see Sigaud col. 1, lines 55-61 and 64-65, col. 2, lines 6-19, col. 3, lines 11-18, col. 4, lines 52-59, and col. 5, line 8, 16-18, 24-26, 33-37, and 47-48). Also, Sigaud discloses that server-1 30 is located within the same enclosure as security processor 1 (col. 3, lines 25-28). A security processor 1 located within the same enclosure as server 30, which Sigaud discloses to be remotely located with respect to user stations 2, cannot reasonably be characterized as a local client terminal that an end user operates, as proposed in the Advisory Action. Thus, the Advisory Action mis-characterizes the relationship between the two devices disclosed by Sigaud as local whereas Sigaud uniformly characterizes it as remote. The Advisory Action has ignored the polar opposite meanings of these words.

Moreover, even if it were assumed, *arguendo*, that Sigaud's security processor and client terminals were co-located, a skilled artisan would recognize the term "client" to refer to a terminal that a user operates to gain access to a server through a network.

Sigaud expressly discloses a security processor 1 interposed between user stations 2 and an application server 30 (Sigaud abstract and each independent claim). Sigaud also discloses that security processor 1 has an initialization file that allows security "processor 1 to close the security connection established with a client station" (Sigaud col. 6, lines 15-24). Accordingly, Sigaud's explicit description of the system precludes the interpretation proposed in the Advisory Action that security processor 1 is a client terminal.

The Advisory Action also proposes that Sigaud discloses storing a predetermined authentication policy in a smart card 22 and an application server-1 30, which the Advisory Action characterizes as the claimed authentication server (Advisory Action section 2, lines 8 and 13-15). By contrast to this proposal however, Sigaud actually discloses that security processor 1 and user station 2 share and execute the authentication policy.

Specifically, Sigaud discloses that a user connects to a protected network by indicating the IP address of security processor 1 and the port number assigned to the application he wishes to use (Sigaud col. 4, lines 28-31). Security processor 1 searches in a table for a security script associated with the port number sent by user station 2 and then establishes a communication with a security application 27, contained in user station 2, so as

to implement the security script for authenticating a portable user object 22 and the identification of the user through his PIN (col. 4, lines 33-39, and col. 2, lines 54-55). Sigaud further discloses that security application 27 is software stored within user station 2 (see col. 6, line 15, Fig. 1, and col. 2, lines 54-55) and that the security script is contained in a table 161 stored by security processor 1 (col. 4, lines 63-65).

Accordingly, Sigaud's explicit description of the system eliminates the prospect that the authentication policy is stored in application server-1 30 and portable user object 22, as proposed in the Advisory Action. Although portable user object 22 may contain information used by an authentication policy, Sigaud expressly states, and illustrates in Fig. 1, that software security application 27 is stored in user station 2, rather than portable user object 22 as proposed in the Advisory Action. Similarly, security processor 1 shares the authentication policy of software security application 27, but application server-1 30 does not.

The comments provided in section 3 of the Advisory Action seem to inadvertently crystallize the distinction between the subject matter defined by claim 40 and that disclosed by Sigaud. Sigaud discloses that a client station and an authentication processor execute a shared authentication process, rather than a PSD and an authentication processor executing this process in accordance with

a user activation on the client station, as recited in claim 40.

And whether evaluated according to: (1) the opposing meanings of "remote" and "local," (2) the conventional meaning attributed to "client" by a skilled artisan in the relevant field, or (3) Sigaud's expressly disclosed distinction between security processor 1 and the "client" user station 2, the Advisory Action's proposal that security processor 1 is a local client terminal that a user operates to gain access to server-1 30 is unfounded. Sigaud expressly states that application server-1 30 and security processor 1 are enclosed within the same enclosure and remotely located with respect to the plurality of user stations 2. A user never has contact with Sigaud's security processor 1 and is only aware of its existence to the extent that something regulates his access to the content of application server-1 30. Whether the functionality of security processor 1 is provided by a tangible component (e.g., hardware) or an intangible component (e.g., software) is irrelevant to the user, since he interfaces to the system through a tangible user station 2. As a result, a security application module (SAM) 151 within Sigaud's security processor 1 necessarily cannot activate an authentication operation upon an action of a user <u>on</u> security processor 1, as proposed in the Advisory Action (see Advisory Action section 2, lines 15-17). Simply stated, a user may act upon user station 2 in Sigaud's

system but cannot act on security processor 1.

In accordance with the above discussion, the Appellants respectfully submit that Sigaud does not anticipate the subject matter defined by claim 40. More specifically, Sigaud does not disclose the claimed feature of a local client that activates an authentication operation, according to an authentication policy shared and stored by a PSD and an authentication server, upon an action of a user on the local client. Therefore, for at least the above resons, reversal of the rejection of claim 40 and its dependent claims is warranted.

Moreover, the dependent claims recite subject matter that provides an independent basis for their individual allowability. The applied art fails to teach or suggest at least the following subject matter of the dependent claims. Claim 41 is allowable for the further reason that it recites that the at least one local client is configured to support at least one device connection, and the intelligent portable device is functionally connected to the at least one local client through the at least one device connection of the at least one local client and further configured as a hardware device peripheral which allows the PSD to communicate the authentication information to the at least one authentication server using the at least one network connection of the at least one local client. Claim 42 is allowable for the further reason that

it recites that the device connection between the at least one local client and the intelligent portable device is selected from the group consisting of a direct connection, an optical connection, a wireless RF connection or an electro-acoustical connection. Claim 43 is allowable for the further reason that it recites that the predetermined authentication policy includes asynchronous authentication means, synchronous authentication means and cryptography means. Claim 44 allowable for the further reason that it recites that the system further comprises at least two local clients respectively functionally connected to at least two authentication servers over at least one network connection, wherein each of the at least two local clients is configured to support at least one device connection, and wherein the intelligent portable device is functionally connected to each of the at least two local clients through the at least one device connection of each of the at least two local clients and further configured as a hardware device peripheral. Claim 45 allowable for the further reason that it recites that the intelligent portable device is functionally connected to the at least one authentication server through at least one network connection and configured as an independent portable device which allows the PSD to communicate the authentication information to the at least one authentication server using the at least one network connection. Claim 46

allowable for the further reason that it recites that the at least one network connection between the at least one authentication server and the intelligent portable device is selected from the group consisting of a wireless RF network and a digital cellular network. Claim 47 is allowable for the further reason that it recites that the intelligent portable device is functionally connected to the at least one authentication server through at least two network connections over at least two networks, a first network connection being dedicated for sending a first portion of the authentication information and a second network connection being dedicated for sending a second portion of the authentication information. Claim 48 is allowable for the further reason that it recites that a plurality of network and device connections are facilitated using the intelligent portable device. Claim 49 is allowable for the further reason that it recites that the intelligent portable device is configured as a hardware device peripheral. Claim 50 is allowable for the further reason that it recites that the intelligent portable device is configured as an independent intelligent portable device. Claim 51 is allowable for the further reason that it recites that the predetermined authentication policy includes asynchronous authentication means and cryptography means. And claim 52 is allowable for the further reason that it recites that the predetermined authentication policy

includes synchronous authentication means and cryptography means.

B. Rejections of Claims 53-64

Appellants respectfully submit that Sigaud fails to disclose at least the features recited in independent claim 53 of performing authentications and business transactions by networking an intelligent portable device configured to support a functionally connected personal security device (PSD), to at least one authentication server using a network connection, wherein a shared predetermined authentication policy is functionally stored in the at least one authentication server and the PSD; initiating an authentication request by an identified user on at least one local client, wherein the identified user is associated with the PSD; sending the request to the at least one authentication server, wherein the at least one local client and the at least one authentication server are functionally connected to each other by a network; authenticating the identified user using the predetermined authentication policy between the PSD and the at least one authentication server; and allowing the identified user access to the network following successful authentication for purposes of performing additional transactions.

Sigaud fails to teach or suggest initiating an authentication request by an identified user on at least one local client, wherein

the identified user is associated with a PSD, according to an authentication policy shared and stored by the PSD and an authentication server.

Accordingly, independent claim 53 distinguishes over Sigaud. Therefore, for at least the above reasons, reversal of the rejections applied to claim 53 and its dependent claims is warranted.

Moreover, the dependent claims recite subject matter that provides an independent basis for their individual allowability. The applied art fails to teach or suggest at least the following subject matter of the dependent claims. Claim 54 is allowable for the further reason that it recites that the authentication request includes at least one unique identifier associated with the identified user. Claim 55 is allowable for the further reason that it recites that the at least one unique identifier is used by the at least one authentication server for locating and communicating with the intelligent portable device associated with the identified user. Claim 56 is allowable for the further reason that it recites that the at least one unique identifier is used by the at least one authentication server for locating and communicating with another intelligent portable device associated with a second level approver. 57 is allowable for the further reason that it recites that a plurality of authentications are facilitated using the

shared predetermined authentication policy. Claim 58 is allowable for the further reason that it recites authentication of the identified user to the PSD by entry of a Personal Identification Number. Claim 59 is allowable for the further reason that it recites authentication of the identified user to the PSD by entry of a biometric result. Claim 60 is allowable for the further reason that it recites that the entry is conducted using a user interface and display associated with the intelligent portable device. Claim 61 is allowable for the further reason that it recites that the entry is conducted using a user interface and display associated with the at least one local client. Claim 62 is allowable for the further reason that it recites that exceeding a maximum number of attempts at authentication ends the authentication. Claim 63 is allowable for the further reason that it recites that the shared predetermined authentication policy includes asynchronous authentication and cryptography, and wherein exceeding a predetermined response time ends the authentication. Claim 64 is allowable for the further reason that it recites business transactions.

C. Rejections of Claims 65-71

To anticipate a claim, an applied reference must disclose every element and its identical arrangement with all other elements

as defined in the claim. See MPEP §2131, last paragraph; *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); and *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The Appellants respectfully submit that Sigaud fails to disclose the feature recited in claim 65 of a personal security device (PSD) that executes an authentication policy, shared with an authentication server, upon receiving a request identifying the user associated with the PSD. Although the discussion provided above in connection with claim 40 is similarly relevant to distinguishing claim 65 from Sigaud and is incorporated here by reference, the Appellants provide a more focused discussion directed to the specific features recited in claim 65, below.

The Advisory Action proposes that the claimed PSD corresponds to Sigaud's smart card and further proposes that Sigaud's disclosure in column 3, lines 30-34, establishes the basis for the proposed correspondence (Advisory Action section 2, lines 10-11). In the cited portion of the specification, Sigaud discloses that "[e]ach of the terminals 2 is equipped with a security application constituted by a piece of software 27 and a physical link 20 with a reader 21 of portable objects 22. These portable objects can be chip cards or PC/MCIA cards." A comparison of the cited disclosure with the Advisory Action's proposal reinforces the inference that

the smart card denominated in the Advisory Action refers to Sigaud's disclosed portable user object 22, which may be a chip card or PCMCIA card.

As discussed in connection with claim 40, Sigaud discloses in Fig. 1 that a user connects to a protected network, via a user station 2, by indicating the IP address of a security processor 1 and the port number assigned to the application he wishes to use (Sigaud col. 4, lines 28-31). Security processor 1 searches in a table for a security script associated with the port number sent by user station 2 and then establishes a communication with a security application 27, contained in user station 2, so as to implement the security script for authenticating a portable user object 22 and the identification of the user through his PIN (col. 4, lines 33-39, and col. 2, lines 54-55).

Security application 27 operates with an operating system of the window-display type, such as Windows® software (col. 4, lines 16-19). Once security software 27 is executed, user station 2 displays a main window (see Fig. 2F) that enables a user of the terminal to activate a security connection with application server-1 30, deactivate the security connection, or exit from the application (col. 4, lines 19-25).

Accordingly, Sigaud's explicit description of the system eliminates the prospect that the authentication policy is executed

in portable user object 22, as proposed in the Advisory Action. Although portable user object 22 may contain information used by an authentication policy, Sigaud expressly states that software security application 27 is executed by user station 2, rather than portable user object 22 as proposed in the Advisory Action.

In accordance with the above discussion, the Appellants respectfully submit that Sigaud does not anticipate the subject matter defined by claim 65. More specifically, Sigaud does not disclose the claimed feature of a PSD that executes an authentication policy, shared with an authentication server, upon receiving a request identifying the user associated with the PSD. Therefore, reversal of the rejection of claim 40 and its dependent claims is warranted.

Moreover, the dependent claims recite subject matter that provides an independent basis for their individual allowability. The applied art fails to teach or suggest at least the following subject matter of the dependent claims. Claim 66 is allowable for the further reason that it recites the feature of being functionally connected to at least one local client using the at least one device connection. Claim 67 is allowable for the further reason that it recites the feature of being functionally connected to at least one authentication server using the at least one network connection. Claim 68 is allowable for the further reason

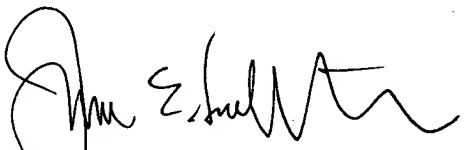
that it recites the feature of being functionally connected to a plurality of local clients using the at least one device connection. Claim 69 is allowable for the further reason that it recites the feature of being functionally connected to a plurality of authentication servers using the at least one network connection. Claim 70 is allowable for the further reason that it recites that the PSD is a physical device. Claim 71 is allowable for the further reason that it recites that the PSD is a virtual device.

VIII. CONCLUSION

In view of the law and facts stated herein, it is respectfully submitted that all pending claims define patentable subject matter.

Therefore, reversal of all outstanding grounds of rejections is respectfully solicited.

Respectfully submitted,



Date: May 1, 2006

James E. Ledbetter
Registration No. 28,732

JEL/att
ATTORNEY DOCKET NO. L741.01104

STEVENS, DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
Washington, D.C. 20036
Telephone: (202) 408-5100
Facsimile: (202) 408-5200

IX. APPENDIX: THE CLAIMS ON APPEAL

40. A data processing system for performing authentications and business transactions comprising:

at least one local client configured to support at least one network connection;

at least one authentication server configured to perform authentications according to a predetermined authentication policy and further configured to support at least one network connection;

an intelligent portable device configured to support a personal security device (PSD), at least one device connection and at least one network connection; and

a PSD which is functionally connected to said intelligent portable device and configured to generate authentication information according to said predetermined authentication policy, and which is associated to an identified user, wherein:

said at least one local client and said at least one authentication server are functionally connected to each other over at least one network connection,

said predetermined authentication policy is functionally stored within said PSD and said at least one authentication server, and

said at least one local client comprises an activator of an authentication according to said authentication policy between said PSD and said at least one authentication server upon an action of said identified user on said at least one local client.

41. The data processing system according to claim 40, wherein:

said at least one local client is configured to support at least one device connection; and

said intelligent portable device is functionally connected to said at least one local client through said at least one device connection of said at least one local client and further configured as a hardware device peripheral which allows the PSD to communicate said authentication information to said at least one authentication server using said at least one network connection of said at least one local client.

42. The data processing system according to claim 41, wherein said device connection between said at least one local client and said intelligent portable device is selected from the group consisting of a direct connection, an optical connection, a wireless RF connection or an electro-acoustical connection.

43. The data processing system according to claim 40, wherein said predetermined authentication policy includes asynchronous authentication means, synchronous authentication means and cryptography means.

44. The data processing system according to claim 40, comprising at least two local clients respectively functionally connected to at least two authentication servers over at least one network connection, wherein each of said at least two local clients is configured to support at least one device connection, and wherein said intelligent portable device is functionally connected to each of said at least two local clients through said at least one device connection of each of said at least two local clients and further configured as a hardware device peripheral.

45. The data processing system according to claim 40, wherein said intelligent portable device is functionally connected to said at least one authentication server through at least one network connection and configured as an independent portable device which allows the PSD to communicate said authentication information to said at least one authentication server using said at least one network connection.

46. The data processing system according to claim 45, wherein said at least one network connection between said at least one authentication server and said intelligent portable device is selected from the group consisting of a wireless RF network and a digital cellular network.

47. The data processing system according to claim 45, wherein said intelligent portable device is functionally connected to said at least one authentication server through at least two network connections over at least two networks, a first network connection being dedicated for sending a first portion of said authentication information and a second network connection being dedicated for sending a second portion of said authentication information.

48. The data processing system according to claim 40, wherein a plurality of network and device connections are facilitated using said intelligent portable device.

49. The data processing system according to claim 40, wherein said intelligent portable device is configured as a hardware device peripheral.

50. The data processing system according to claim 40, wherein said intelligent portable device is configured as an independent intelligent portable device.

51. The data processing system according to claim 40, wherein said predetermined authentication policy includes asynchronous authentication means and cryptography means.

52. The data processing system according to claim 40, wherein said predetermined authentication policy includes synchronous authentication means and cryptography means.

53. A method for performing authentications and business transactions comprising:

networking an intelligent portable device configured to support a functionally connected personal security device (PSD), to at least one authentication server using a network connection, wherein a shared predetermined authentication policy is functionally stored in said at least one authentication server and said PSD;

initiating an authentication request by an identified user on at least one local client, wherein said identified user is associated with said PSD;

sending the request to said at least one authentication server, wherein said at least one local client and said at least one authentication server are functionally connected to each other by a network;

authenticating said identified user using said predetermined authentication policy between said PSD and said at least one authentication server; and

allowing said identified user access to the network following successful authentication for purposes of performing additional transactions.

54. The method according to claim 53, wherein said authentication request includes at least one unique identifier associated with said identified user.

55. The method according to claim 54, wherein said at least one unique identifier is used by said at least one authentication server for locating and communicating with said intelligent portable device associated with said identified user.

56. The method according to claim 54, wherein said at least one unique identifier is used by said at least one authentication server for locating and communicating with another intelligent

portable device associated with a second level approver.

57. The method according to claim 53, wherein a plurality of authentications are facilitated using said shared predetermined authentication policy.

58. The method according to claim 53, further comprising an authentication of said identified user to said PSD by entry of a Personal Identification Number.

59. The method according to claim 53, further comprising an authentication of said identified user to said PSD by entry of a biometric result.

60. The method according to claim 58 or 59, wherein said entry is conducted using a user interface and display associated with said intelligent portable device.

61. The method according to claim 58 or 59, wherein said entry is conducted using a user interface and display associated with said at least one local client.

62. The method according to claim 58 or 59, wherein

exceeding a maximum number of attempts at authentication ends the authentication.

63. The method according to claim 53, wherein said shared predetermined authentication policy includes asynchronous authentication and cryptography, and wherein exceeding a predetermined response time ends the authentication.

64. The method according to claim 53, further comprising business transactions.

65. An intelligent portable data processing device for performing authentications and business transactions comprising a user interface, a display, data processing means, data storage means, at least one device connection and at least one network connection, further comprising:

a personal security device (PSD) configured to generate authentication information according to a predetermined authentication policy which is shared with at least one remote authentication server, wherein said PSD is associated to an identified user; and

means for transferring to the PSD a request for authentication with said at least one authentication server,

using said shared predetermined authentication policy, upon reception of said request, if said request contains an identifier of said identified user.

66. The intelligent portable data processing device according to claim 65, functionally connected to at least one local client using said at least one device connection.

67. The intelligent portable data processing device according to claim 65 or 66, functionally connected to at least one authentication server using said at least one network connection.

68. The intelligent portable data processing device according to claim 65, functionally connected to a plurality of local clients using said at least one device connection.

69. The intelligent portable data processing device according to claim 65 or 68, functionally connected to a plurality of authentication servers using said at least one network connection.

70. The intelligent portable data processing device

according to claim 65, wherein the PSD is a physical device.

71. The intelligent portable data processing device according to claim 65, wherein the PSD is a virtual device.